amount of work required to invert, compared to the cost of calculation of the output of the function. The application of this invention to key escrowing is described. A basic algorithm for implementation as an example of a suitable limited one-way function is described. This problem involves randomization and can be viewed as an extension of the puzzling problem originally developed by Ralph C. Merkle, "Secure Communications Over Insecure Channels," Communications of the ACM, April 1978, Volume 21, Number 4, pages 294-299. The basic algorithm utilized in implementation of the invention requires a randomized response and achieves a limited, but measurable computational advantage of the data receiver over an eavesdropper. Algorithm performance and application to the implementation of a delay function for employment in key escrow systems is hereinafter explained.

IN THE CLAIMS:

For the convenience of the Examiner, all pending claims are shown below whether or not an amendment has been made.

1. (Amended) A method for storing and withdrawing a decryption key from a key escrow database, comprising:

creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token;

transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver;

randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token;

adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair;

encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair;

recording in a key escrow database the created set of N trap door encryption-decryption function pairs and the corresponding paired token;